拡張Hensel構成を用いた多変数多項式の因数分解

AUTHOR(S):

稲葉, 大樹

CITATION:

稲葉, 大樹. 拡張Hensel構成を用いた多変数多項式の因数分解. 数理解析研究所講究録 2004, 1395: 111-118

ISSUE DATE:

2004-10

URL:

http://hdl.handle.net/2433/25935

数理解析研究所講究録 1395 巻 2004 年 111-118

拡張Hensel構成を用いた多変数多項式の因数分解

稲葉 大樹

DAIJU INABA

筑波大学 数学研究科

DOCTORAL PROGRAM IN MATHEMATICS, UNIVERSITY OF TSUKUBA *

Abstract

拡張 Hensel 構成とは、展開点が特異点で非零代入を行わない Hensel 構成である。本稿では主係数問題への対応を行った拡張 Hensel 構成を用いた多変数多項式の因数分解法を計算機に実装し、一般 Hensel 構成において非零代入により項数増大が起こる多変数多項式の因数分解が効率良く行えるかどうかを検証する。

1 はじめに

$\mathbf{K}$ を数体とし、$F(x,u_1,\ldots,u_\ell)$ を $\mathbf{K}$ 上の無平方である多項式とし、$\bar{\mathbf{K}}$ を $\mathbf{K}$ の代数的閉包とする。また、$(s_1,\ldots,s_\ell)$ を Hensel 構成の展開点とする。

一般 Hensel 構成において $F(x,s_1,\ldots,s_\ell)$ が無平方でない場合、$(s_1,\ldots,s_\ell)$ を Hensel 構成の特異点といい、$F(x,u_1,\ldots,u_\ell)$ の主係数が $(s_1,\ldots,s_\ell)$ で 0 になるとき、$(s_1,\ldots,s_\ell)$ で主係数が特異であるという。

多変数多項式の一般 Hensel 構成の主な応用の一つとして多変数多項式の因数分解が挙げられる。基本的に展開点を原点として Hensel 構成を行うことにより、因数分解に必要な Hensel 因子が得られる。

しかし、原点が特異点もしくは原点で主係数が特異である場合、一般 Hensel 構成は破綻する。このとき、展開点を変更する必要がある。実際の計算では展開点により多項式の平行移動を行う (これを非零代入という) が、多項式によってはこれを行うことにより平行移動後の多項式の項数が爆発的に増加する場合があり、これにより Hensel 構成に時間がかかってしまう。これを非零代入問題という。

展開点が特異点である場合の Hensel 構成について 2 変数多項式に対しては 1989 年に Kuo により [Kuo89]、多変数多項式に対しては 1993 年に Sasaki と Kako により [SK99]、考案された。この方法を Sasaki と Kako は 拡張 Hensel 構成と命名した。さらに、Sasaki と Inaba は主係数が特異である場合にも適用できるように Sasaki-Kako の方法を拡張し、拡張 Hensel 構成を用いた多変数多項式の因数分解の方法も提案した [SI00]。

しかし、実際に拡張 Hensel 構成を用いた多変数多項式の因数分解法を実装するにあたって、解決すべき問題が残されていた。それは主係数問題である。一般 Hensel 構成においては Wang [Wan77] など、多くの人により解決されている。

本稿では 2 章で拡張 Hensel 構成とそれを構成を用いた因数分解法の概要 (詳細は [SK99], [SI00] を参照されたい) を紹介し、3 章では拡張 Hensel 構成における主係数問題の解決策を述べる。4 章では拡張 Hensel 構成を用いた多変数多項式の因数分解法を実装し、その効率性を従来の一般 Hensel 構成を用いた方法と比較、検証する。

2 拡張Hensel構成と因数分解

$\mathbf{K}$ を数体とし、$\bar{\mathbf{K}}$ を $\mathbf{K}$ の代数的閉包とする。$\mathbf{K}[u_1,\ldots,u_\ell]$, $\mathbf{K}(u_1,\ldots,u_\ell)$ と $\mathbf{K}\{u_1,\ldots,u_\ell\}$ をそれぞれ $\mathbf{K}$ 上 $u_1,\ldots,u_\ell$ を変数とする多項式環、有理式体、形式的べき級数環とする。$(s_1,\ldots,s_\ell)\in\bar{\mathbf{K}}^\ell$ とし、$(u_1,\ldots,u_\ell)$ と $(s_1,\ldots,s_\ell)$ をそれぞれ (u) と (s) と略記する。多項式 $F(x,u)\in\mathbf{K}[x,u]$ は無平方 (重複因子が存在しない) で各変数について原始的 (係数が互いに素) であるとし、

$$F(x,u)=f_n(u)x^n+f_{n-1}(u)x^{n-1}+\cdots+f_0(u)x^0,\quad f_n(u)\neq 0 \tag{1}$$

*inaba@math.tsukuba.ac.jp

と表記する。$\deg(F)$, $\mathrm{lc}(F)$ をそれぞれ多項式 F の x に関する次数、主係数とする。$\mathrm{tdeg}(f_i)$ を各 f_i の $u_1,\ldots,u_\ell$ に関する全次数 (f_i の各項 $T = cu_1^{e_1}\cdots u_\ell^{e_\ell}$ $(c \neq 0)$ に対し、その全次数 $\mathrm{tdeg}(T) = e_1 + \cdots + e_\ell$ の最大をとる) とする。$\mathrm{ord}(f_i)$ を f_i の各項の全次数のうち最小のものとし、これを f_i の位数という。また、有理関数 $f(u)/g(u)$ に関して、その位数を $\mathrm{ord}(f/g) = \mathrm{ord}(f) - \mathrm{ord}(g)$ で定義する。$\gcd(F,G)$ を多項式 F と G の最大公約数とし、$\mathrm{cont}(F) = \gcd(f_n, f_{n-1}, \cdots, f_0)$ を $F(x,u)$ の係因数とする。

u の有理式 $G(u)$ が以下のように分解されるものとする。

$$\begin{cases} G(u) = g_0(u)/d_0(u) + g_1(u)/d_1(u) + \cdots + g_k(u)/d_k(u) + \cdots \\ \qquad g_k(u) \text{ と } d_k(u) \text{ は } \bar{\mathbf{K}}[u] \text{ に関して同次式} \\ \qquad \mathrm{ord}(g_k/d_k) = k \quad (k = 0,1,2,\ldots) \end{cases} \tag{2}$$

$\bar{\mathbf{K}}\{(u)\}$ を (2) のような負でない位数から成る同次有理式の級数環とする。

定義 1 (特異点、主係数が特異)
展開点 (s) に対し、$F(x,s)$ が無平方でないとき、(s) を (Hensel 構成の) 特異点という。また、$f_n(s) = 0$ をみたすとき、(s) で主係数が特異であるという。

まず、従変数 $u_1,\ldots,u_\ell$ の全次数変数 t を $u_i \mapsto tu_i$ $(i = 1,\ldots,\ell)$ という変換で導入する。(または、$u_i \mapsto t^{\omega_i}u_i$ $(i = 1,\ldots,\ell)$、$(\omega_1,\ldots,\omega_\ell$ は正の数) と、重みをつけて導入してもよい。) 全次数変数導入後の多項式を $\hat{F}(x,t,u)$ とする。

定義 2 ($F(x,u)$ の Newton 線 $\mathcal{L}$ と Newton 多項式 $F_{\mathrm{New}}(x,u)$)
0 でない $\hat{F}(x,t,u)$ の各項 $cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}$ $(c \in \mathbf{K},\ j = j_1 + \cdots + j_\ell)$ に対応する点 (i,j) を (e_x,e_t)-平面にプロットする。$\nu = \mathrm{ord}(f_n)$ とし、点 (n,ν) (図 1 では点 P を指す) を通る (e_x,e_t)-平面上の直線のうち、他の少なくとも一点を通り、直線より下にはプロットが存在しないものを $F(x,u)$ の Newton 線 ($\mathcal{L}$ と表記) と定義する。$\mathcal{L}_{\mathrm{New}}$ 上にあるプロットに対応する全ての項の和を $F(x,u)$ の Newton 多項式 ($F_{\mathrm{New}}(x,u)$ と表記) と定義する。

例 1
以下の多項式 F を考える。

$$\begin{aligned} F(x,y,z) = {} & x^4(y^2-z^2) + x^3(y+3z+3y^2+3z^2) \\ & + x^2(-2+3y-4z-2y^2+5yz-2z^2+y^3+6y^2z+3z^3) \\ & + x^1(-5y-9y^2-5yz-5z^2+3y^3+y^2z-5z^3) \\ & + (3y^2-5y^3-7y^2z-yz^2-2y^4-3y^2z^2-3yz^3-2z^4). \end{aligned}$$

$F(x,y,z)$ の各項のプロットは右図で、Newton 多項式 $F_{\mathrm{New}}(x,y,z)$ は下式となる。

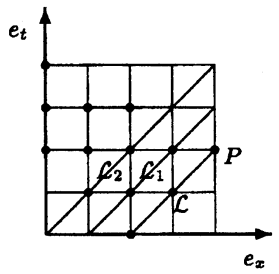


図 1

$$\begin{aligned} F_{\mathrm{New}} &= x^4(y^2-z^2) + x^3(y+3z) - 2x^2 \\ &= x^2\cdot[x(y-z)+2]\cdot[x(y+z)-1]. \quad \square \end{aligned}$$

F_{New} を互いに素な因子 $G_1^{(0)},\ldots,G_r^{(0)}$ に分解し、これらの因子を初期因子として

$$F(x,u) \equiv G_1^{(k)}(x,u)\cdots G_r^{(k)}(x,u) \pmod{I_{k+1}}. \tag{3}$$

となるように分解するのが拡張 Hensel 構成である。ここでイデアル I_k は上記で $k = 0 \Rightarrow 1 \Rightarrow 2 \Rightarrow \cdots$ と上げていくとき、新たに取り込まれる項を通る直線 $\mathcal{L}_k$ が $\mathcal{L}$ に平行のまま上にシフトし、かつ全てのプロット点を走査するように決める。

定義 3 ($G(x,u)$ の Newton 多角形)
$G(x,u) \in \bar{\mathbf{K}}\{(u)\}[x]$ において $G(x,tu)$ の各項 $cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}/D(tu)$ $(c \in \bar{\mathbf{K}},\ j = j_1 + \cdots + j_\ell,\ D(u)$ は $\mathrm{ord}(D) = d$ を満たす $u_1,\ldots,u_\ell$ についての同次多項式) に対応する点 $(i,\ j-d)$ を (e_x,e_t)-平面にプロットする。このとき、$G(x,u)$ の Newton 多角形 $\mathcal{N}$ はプロットされた全ての点に対する凸包と定義する。さらに $\mathcal{N}$ の下辺を時計回りに $S_1,\ldots,S_\rho$ とする。

Newton 線は最右側の下辺である $\mathcal{S}_1$ に過ぎない。図 2 は例 1 の多項式における Newton 多角形で、この場合図 2 の $\mathcal{S}_1, \mathcal{S}_2$ が下辺である。
Newton 多角形の下辺が 1 本、つまり $\rho = 1$ であるとき、拡張 Hensel 構成は 1 回で済む。この場合は一般 Hensel 構成と同様に Hensel 因子に分解できる。以下、$\rho > 1$ の場合について述べる。まず、$F(x,u)$ の Newton 多項式 $F_{\mathcal{S}_1}$ を以下の通りに分解する (下記の n_1 は $F_{\mathcal{S}_1}$ の最小次数)。

$$F_{\mathcal{S}_1} = x^{n_1} \cdot \mathrm{cont}(F_{\mathcal{S}_1}) G_1^{(0)}(x,u) \cdots G_r^{(0)}(x,u). \tag{4}$$

ただし、$x^{n_1}, G_1^{(0)}, \ldots, G_r^{(0)}$ は互いに素であるとする。これらを初期因子として拡張 Hensel 構成を行うと $F(x,u)$ は以下の通りに分解できる。

$$F(x,u) = F_2(x,u) \cdot \mathrm{cont}(F_{\mathcal{S}_1}) G_1^{(\infty)}(x,u) \cdots G_r^{(\infty)}(x,u). \tag{5}$$

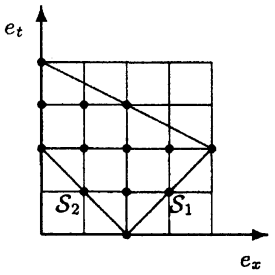


図 2：Newton 多角形の例

ここで、$F_2(x,u)$ は x^{n_1} に対応する Hensel 因子であるが、この $F_2(x,u)$ に再び拡張 Hensel 構成を適用する (Newton 線は $\mathcal{S}_2$) ことで Hensel 因子に分解できる。以上を繰り返すことにより、$\mathcal{S}_1 \Rightarrow \mathcal{S}_2 \Rightarrow \cdots \Rightarrow \mathcal{S}_\rho$ の順に Hensel 因子を得ることができる。ただし、得られる Hensel 因子は [SI00] の Theorem 1 (分解定理) より $\bar{\mathbf{K}}\{u\}[x]$ ではなく $\bar{\mathbf{K}}\{(u)\}[x]$ 内の式になる。

次に因子の組み合わせについて述べる。まず $\bar{\mathbf{K}}\{(u)\}[x]$ 内のいくつかの既約因子をかけることで $\bar{\mathbf{K}}\{u\}[x]$ 内の既約因子を作るが、これは以下の方法で行う。

1. まず、各 $i \in \{1, \ldots, \rho\}$ に対し、$\mathcal{S}_i$ 上に対応する Hensel 因子同士で固有の分母因子 $d_i(u)$ を持つとき、それらを組み合わせて分母 $d_i(u)$ を消去する (この方法は拡張 Hensel 構成の計算途中で行うことができる)。
2. 次に $\mathcal{S}_1, \ldots, \mathcal{S}_\rho$ 内で異なる辺上の Hensel 因子が固有の分母因子を持てば、それらを組み合わせてその分母を消去する。

上記の組み合わせが終了した後、生成した $\bar{\mathbf{K}}\{u\}[x]$ 内のいくつかの既約因子をかけることで $\bar{\mathbf{K}}[x,u]$ 内の既約因子を作る。

3 拡張 Hensel 構成と主係数問題

拡張 Hensel 構成を用いて多変数多項式を因数分解する際生じる主係数問題の解決策を提案する。ここでの多項式 $F(x,u)$ は原点 $(u) = (0)$ が特異点であることを仮定する。まず、F_{New} の Newton 多項式 F_{New} を $\bar{\mathbf{K}}[x,u]$ 上で以下の通りに因数分解する。

$$\begin{cases} F_{\mathrm{New}}(x,u) = G_0^{(0)}(x,u) \cdot G_1^{(0)}(x,u) \cdots G_r^{(0)}(x,u), \\ G_0^{(0)} = \mathrm{cont}(F_{\mathrm{New}})\, x^{n_0}, \quad \gcd(G_i^{(0)}, G_j^{(0)}) = 1 \ \ (\forall i \neq j). \end{cases} \tag{6}$$

上記の n_0 は F_{New} の最小の次数とする。次に、$F(x,u)$ の主係数 $f_n(u)$ も同様に $\bar{\mathbf{K}}[u]$ 上で因数分解する。

$$\begin{cases} f_n(u) = w \cdot W_1(u)^{t_1} \cdots W_s(u)^{t_s}, \\ w \in \bar{\mathbf{K}}, \ \ \gcd(W_i, W_j) = 1 \ \ (\forall i \neq j). \end{cases} \tag{7}$$

一般 Hensel 構成における主係数問題の解決策の 1 つとして Wang が [Wan77] 主係数を因数分解し、その因子を Hensel 構成の初期因子に適切に割り振り、各々の主係数に置き換えて Hensel 構成を行うという方法を提案した。拡張 Hensel 構成でも同様に 上記の $W_1, \ldots, W_s$ を $G_i^{(0)}$ $(i = 0, \ldots, r)$ に振り分けたい。しかし、 Wang の方法は展開点が特異点の場合は展開点を変更する場合がある。従って、 Wang の方法は拡張 Hensel 構成では使えない。そこで "principal terms" を定義する。

定義 4 (principal terms)
多項式 $f(u)$ に対し、 その principal terms を位数が $\mathrm{ord}(f)$ である項の総和として定義し、これを $\mathrm{pt}(f)$ と表記する。有理式 $f(u)/g(u)$ に対しては、$\mathrm{pt}(f/g) = \mathrm{pt}(f)/\mathrm{pt}(g)$ と定義する。尚、principal terms に関して、乗法 $\mathrm{pt}(f \cdot g) = \mathrm{pt}(f) \cdot \mathrm{pt}(g)$ は明らかに成り立つ。

例 2
principal terms の例

$$\begin{array}{lll} g_1 = 3u_1^2 - 4u_1u_2 + 5u_2^2 - 6u_1 + 5u_2 & : & \mathrm{pt}(g_1) = -6u_1 + 5u_2, \\ g_2 = 3u_1^6 - 2u_2^3 + 1 & : & \mathrm{pt}(g_2) = 1, \\ g_3 = (6u_1^5 - 5u_2^4 + 4u_1^2)/(u_1^2 + u_2) & : & \mathrm{pt}(g_3) = 4u_1^2/u_2. \end{array} \quad \square$$

Newton 多項式を以下の通りに表す。

$$F_{\mathrm{New}}(x,u)=\mathrm{pt}(f_n)x^n+\cdots+\mathrm{pt}(f_{n_0})x^{n_0}. \tag{8}$$

すると、(7) と (8) より、

$$\mathrm{lc}(G_0^{(0)})\cdots\mathrm{lc}(G_r^{(0)})=w\ \mathrm{pt}(W_1)^{t_1}\cdots\mathrm{pt}(W_s)^{t_s}.$$

これにより W_j $(j=1,\ldots,r)$ の分配は $\mathrm{pt}(W_i)$ が $\mathrm{lc}(G_0^{(0)}),\ldots,\mathrm{lc}(G_r^{(0)})$ のいずれかを割るかどうかで決定することができる。ところが、ある j に対し、$\mathrm{pt}(W_j)$ が 2 つ以上の $\mathrm{lc}(G_i^{(0)})$ で割る場合、その分配は一意ではなくなる。その場合、W_j を該当する $G_i^{(0)}$ に振り分ける (例 3 参照)。さらに w は $G_0^{(0)}$ に分配する。以上により $G_0^{(0)},\ldots,G_r^{(0)}$ に振り分けられた主係数の因子の積をそれぞれ $C_0,\ldots,C_r$ とする。W_j の分配が一意でないとき、拡張 Hensel 構成の計算は以下の通りにして補完する。

まず、W_j の分配において余分に振り分けられた因子の積を求める。これを $\tilde{f}(u)$ とすると、$\tilde{f}(u)=(C_0\cdots C_r)/f_n$ となる。ここで、$\tilde{F}(x,u)=\tilde{f}(u)\cdot F(x,u)$ とおく。このとき $i=0,\ldots,r$ に対して、$\tilde{G_i^{(0)}}=(\mathrm{pt}(C_i)/\mathrm{lc}(G_i^{(0)}))G_i^{(0)}$ とおけば、$\tilde{F}$ の Newton 多項式 $\tilde{F}_{\mathrm{New}}$ は

$$\tilde{F}_{\mathrm{New}}(x,u)=\tilde{G}_0^{(0)}\cdots\tilde{G}_r^{(0)}. \tag{9}$$

と分解される。そして $i=0,\ldots,r$ に対し、$\tilde{G}_i^{(0)}$ の主係数を C_i に置き換え、それらを初期因子とすることで拡張 Hensel 構成を行い $\tilde{F}(x,u)$ を分解することにより、因数分解に必要な Hensel 因子が得られる。

最後に組み合わされた Hensel 因子に対し、それぞれの係因数を除くことにより、$F(x,u)$ の多項式因子を得ることができる。

例 3
以下の多項式 F を考える。

$$\begin{aligned}F &= x^3(12y^3+8y^2z-yz^2-z^3+2y^3z-3y^2z^2-2yz^3-20y^3z^2+5y^2z^3+6y^3z^3)\\ &\quad+x^2(14y^2-yz-4z^2-6y^3-5y^2z-15yz^2-2z^3\\ &\quad\ +44y^3z-27y^2z^2+2yz^3-20y^3z^2+18y^2z^3+2y^3z^3)\\ &\quad+x(-5z+6y^2-4yz-8z^2-18y^3+33y^2z-14yz^2+5z^3\\ &\quad\ +24y^3z-58y^2z^2+18yz^3+12y^3z^2-9y^2z^3-6y^3z^3)\\ &\quad+(-2+12y-6z-18y^2+6yz+2z^2+42y^2z-36yz^2+6z^3\\ &\quad\ -18y^3z+6y^2z^2+2yz^3+12y^3z^2-6y^2z^3-2y^3z^3).\end{aligned}$$

F の Newton 多角形の下辺は 1 本のみである。Newton 多項式 F_{New} は以下の通りに因数分解される。

$$F_{\mathrm{New}}=[x(3y-z)-1]\cdot[x(2y+z)+2]\cdot[x(2y+z)+1]$$

これより、$G_1^{(0)}=x(3y-z)-1$, $G_2^{(0)}=x(2y+z)+2$, $G_3^{(0)}=x(2y+z)+1$ とする。主係数 $\mathrm{lc}(F)$ も同様に因数分解する。

$$\mathrm{lc}(F)=(-3y+z+yz)(2y+z+3yz)(-2y-z+2yz).$$

$W_1=-3y+z+yz$, $W_2=2y+z+3yz$, $W_3=-2y-z+2yz$ とする。このとき、$\mathrm{pt}(W_1)=-3y+z$, $\mathrm{pt}(W_2)=2y+z$, $\mathrm{pt}(W_3)=-(2y+z)$. $W_1\,|\,\mathrm{lc}(G_1^{(0)})$, $W_1\nmid\mathrm{lc}(G_2^{(0)})$, $W_1\nmid\mathrm{lc}(G_3^{(0)})$ より W_1 は $G_1^{(0)}$ のみに分配される。ところが、$\mathrm{pt}(W_2)=-\mathrm{pt}(W_3)$, W_2 と W_3 は $G_2^{(0)}$ と $G_3^{(0)}$ の両方に分配できる。これより、C_1, C_2, C_3 は以下の通りになる。

$$C_1=W_1,\ C_2=W_2W_3,\ C_3=W_2W_3.$$

次に、$\tilde{F}$ を計算する。

$$\tilde{f}=(C_1C_2C_3)/\mathrm{lc}(F)=W_2W_3,\quad \tilde{F}=\tilde{f}\cdot F=W_2W_3\cdot F.$$

$\tilde{G}_1^{(0)}$, $\tilde{G}_2^{(0)}$, $\tilde{G}_3^{(0)}$ は以下の通りになる。

$$\tilde{G}_1^{(0)}=x(3y-z)-1,\quad \tilde{G}_2^{(0)}=-x(2y+z)^2-2(2y+z),\quad \tilde{G}_3^{(0)}=-x(2y+z)^2-(2y+z).$$

以上を初期因子として、拡張 Hensel 構成を行う。2 次まで構成を行うと、

$$\begin{aligned}\tilde{G_1^{(2)}} &= (-3y+z+yz)x+1-3y+3z+yz,\\ \tilde{G_2^{(2)}} &= [6y^2z^2-yz(2y+z)-(2y+z)^2]x+(-4y-2z-2yz+2z^2-4y^2z+4yz^2-6y^2z^2)\\ &= (3yz+2y+z)[\,(-2y-z+2yz)x-2+2z-2yz],\\ \tilde{G_3^{(2)}} &= [6y^2z^2-yz(2y+z)-(2y+z)^2]x+(-2y-z+6y^2+3yz-z^2-8y^2z+yz^2+2y^2z^2)\\ &= (2yz-2y-z)[\,(2y+z+3yz)x+1-3y+z+yz].\end{aligned}$$

あとは $\tilde{G}_1^{(2)}, \tilde{G}_2^{(2)}, \tilde{G}_3^{(2)}$ の係因数を除くことにより、以下の通りに $F(x,u)$ の多項式因子を得る。

$$F(x,y,z) = [\,(-3y+z+yz)x+1-3y+3z+yz]\cdot[\,(-2y-z+2yz)x-2+2z-2yz]\cdot[\,(2y+z+3yz)x+1-3y+z+yz]$$

□

4 実験

拡張 Hensel 構成を用いた多変数多項式の因数分解法を国産の数式処理システム GAL(General Algebraic Language) に実装し、その効率性を 2 つの実験により、従来の一般 Hensel 構成を用いた方法と比較、検証する。

まずは本実験で使用する 3 種類の多変数多項式の因数分解を紹介する。

- method H
  一般 Hensel 構成を用いて因数分解を行う。Hensel 構成が破綻する展開点に対しては多項式を平行移動させることにより展開点を変更する。また、主係数が定数でない場合、元の多項式を主係数でべき級数除算を行い、さらに各初期因子もそれぞれの主係数で割ることで、それら全ての主係数を 1 に規格化する。
- method W
  method H と同様に一般 Hensel 構成を用いて因数分解を行う。ただし、Wang の方法 [Wan77] を用いて Hensel 構成の初期因子に対し適切に主係数を振り分ける。
- method E
  本稿で紹介した拡張 Hensel 構成を使用して因数分解を行う。

実験 1

実験 1 における実験環境を下に記す。

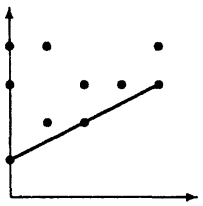
OS	Linux 2.4.22
CPU	AMD Athelon(tm) XP 1900+ (1.60GHz)
Memory	1.00 Gbyte

- method H, W において展開点 $(y,z) = (a,b)$, $(a \neq 0, b \neq 0)$ で一般 Hensel 構成可能
- 主変数に関し (4 次) × (3 次)
- 従変数の全次数は 60 次以下
- 多項式の項数は 60 ~ 80 個
- 数係数は $\{-10,-9,\ldots,9,10\}$ 内でランダム

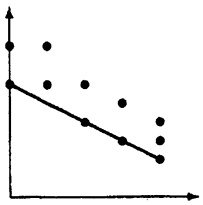
を満たす 3 変数多項式 (主変数 x, 従変数 y,z) で、

(1) Newton 多角形の下辺が 1 本で、その傾きが正のとき
(2) Newton 多角形の下辺が 1 本で、その傾きが負のとき
(3) Newton 多角形の下辺が 2 本のとき

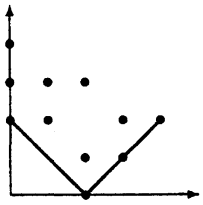
の 3 種の状況下で多項式を各 10 個作成し、それぞれに対し methods H, W, E における平均 CPU 時間 T_H, T_W, T_E を測定した。



実験 1 (1) の場合



実験 1 (2) の場合



実験 1 (3) の場合

T_H (秒)	T_W (秒)	T_E (秒)	T_H/T_E	T_W/T_E
139.0	0.440	0.0900	1540.	4.89
3.38	0.730	0.0590	57.3	12.4
23.7	1.89	0.439	54.0	4.31
2.53	1.08	0.0640	39.5	16.9
45.0	0.250	0.0840	536.	2.97
12.4	0.233	0.0850	33.1	3.65
1.94	0.860	0.0590	32.9	14.6
21.5	1.42	0.461	46.6	3.08
3.97	0.768	0.0610	65.1	12.6
54.7	0.297	0.0940	582.	3.16

表 1: Newton 多角形の下辺が 1 本で、その傾きが正のとき

T_H (秒)	T_W (秒)	T_E (秒)	T_H/T_E	T_W/T_E
1.56	2.24	0.0710	22.0	31.6
39.7	1.79	1.20	33.1	1.49
17.8	0.452	0.0880	202.	5.14
1.31	0.139	0.0210	62.4	6.62
11.6	0.484	0.0820	141.	5.90
1.21	1.63	0.0690	17.5	23.6
48.2	1.04	1.44	33.5	0.722
14.5	0.547	0.0890	163.	6.15
0.870	0.117	0.0240	36.3	4.88
31.0	0.651	0.0980	316.	6.64

表 2: Newton 多角形の下辺が 1 本で、その傾きが負のとき

T_H (秒)	T_W (秒)	T_E (秒)	T_H/T_E	T_W/T_E
0.0450	0.0600	0.145	0.310	0.414
0.791	0.102	0.114	6.94	0.895
0.308	0.0943	0.0424	7.26	2.22
0.376	0.145	0.168	2.24	0.863
0.0900	0.131	0.231	0.390	0.567
1.15	0.104	0.0685	16.8	1.52
0.322	0.319	0.0667	4.83	4.78
0.348	0.0892	0.185	1.88	0.482
0.135	0.0564	0.0548	2.46	1.03
1.09	0.0568	0.0716	15.2	0.793

表 3: Newton 多角形の下辺が 2 本のとき

表 1 ～ 表 3 は上記の実験結果である。各表の T_H, T_W, T_E の単位は秒である。また、右側 2 列の $T_H/T_E, T_W/T_E$ はそれぞれ T_E に対する T_H, T_W の割合である。

まず、表 1 の結果から Newton 線の下辺が 1 本で傾きが正の場合、method H, W より、method E の方が効率良く因数分解が行えることがわかる。実際の計算時間は method E に対して、method W では 約 3 ～ 17 倍, method H では 少なくとも約 30 倍、中には 1000 倍以上のものもあった。method H, W において多項式の平行移動後の項数は元の多項式の項数の約 30 ～ 80 倍になり、それによる Hensel 構成の計算時間への影響が現れたと考えられる。このことから、非零代入を行わない method E の効率性があらわれたといえよう。また、表 2 の結果から傾きが負のときでも同様のことがいえる。したがって、Newton 線の下辺が 1 本のときは傾きの正負に関わらず method E の効率性が表れていることがいえる。なお、method H と method W を比べると method W の方が効率が良い場合が多いが、これは method W では Hensel 構成における初期因子の個数が元の多項式の多項式因子の個数と一致するとき、Hensel 因子がそのまま多項式因子となり得る。それに対し、method H では多項式因子が直接現れず、べき級数として Hensel 因子が計算される。したがって、method W の方が method H より因数分解に必要な Hensel 構成の次数が低くて済む上、組み合わせも必要無い場合が多い。

次に、表 3 の結果から Newton 多角形の下辺が 2 本のとき、method E の効率性は Newton 多角形の下辺が 1 本のときほど現れていないことが分かる。Newton 多角形の下辺が 2 本の場合、method H, W は Hensel 構成 1 回で因数分解可能であることに対し、method E は Hensel 構成が 2 回必要になる。さらに、因数分解に必要な Hensel 因子を得るためには 1 回目の Hensel 構成での次数を method H, W より高く設定する必要がある。したがって、以上で述べた分余計に計算に時間がかかる。このことに関しては改善の余地がある (5 章参照)。

実験 2

実験 2 における実験環境を下に記す。

OS	Linux 2.4.22
CPU	Xeon(TM) 2.80 GHz
Memory	1.00 Gbyte

以下の 3 変数多項式 F_1, F_2 を考える。

$$F_1(x,y,z) = (f_1 \cdot f_2 + 2y^2x + r_1x + r_2)(f_3 \cdot f_4 + zx + r_3x + r_4)$$
$$F_2(x,y,z) = (f_1 \cdot f_2 + r_1x + r_2)(f_3 \cdot f_4 + r_3x + r_4)$$

ただし、f_1, f_2, f_3, f_4, r_i は以下の通りである。

$$f_1 = (y^2+z^2)x + 5y, \quad f_2 = (y+2z)x + 2,$$
$$f_3 = (3y+2z)x + 2, \quad f_4 = (y+6z)x + 2,$$
$$r_i = R_i(y^{e_{i1}}z^{e_{i2}} - y^{e_{i3}}z^{e_{i4}}) \quad (i = 1,2,3,4).$$

F_1, F_2 の各 r_i に対して、$R_1, \ldots, R_4$ は $\{-9, -8, \ldots, 8, 9\}$ 内でランダムに選び、e_i $(i = 1, \ldots, 16)$ は

(1) 全次数 40 前後 ($8 \leq e_i \leq 12$)
(2) 全次数 60 前後 ($13 \leq e_i \leq 17$)

になるようにランダムに選ぶ。以上の条件を満たす多項式を各全次数ごとにそれぞれ 5 個ずつ生成し、因数分解にかかる平均 CPU 時間を測定する。

この F_1, F_2 について共に展開点 $(y, z) = (a, b)$ において $a = 0$ または $b = 0$ のとき (a, b) は特異点になる。そこで method H, W において、展開点を $(y, z) = (1, 1)$ とする。このとき平行移動後の多項式の項数は F_1 では約 16 倍、F_2 では約 36 倍になる。この展開点での method H, W、展開点が原点での method E 全てについて Hensel 構成の初期因子は F_1 では 2 個、F_2 では 4 個になる。また、method E における Newton 多角形の下辺は F_1, F_2 共に 1 本である。

total degree $\simeq$ 40

T_H(秒)	T_W(秒)	T_E(秒)	T_H/T_E	T_W/T_E
0.698	0.194	0.0630	11.1	3.08
0.695	0.273	0.0705	9.86	3.87
0.704	0.155	0.0620	11.4	2.5
0.705	0.166	0.0645	10.9	2.57
0.589	0.140	0.0655	8.99	2.14

total degree $\simeq$ 60

T_H(秒)	T_W(秒)	T_E(秒)	T_H/T_E	T_W/T_E
3.21	0.891	0.0780	41.2	11.4
3.70	0.791	0.0735	50.3	10.8
2.69	0.655	0.0740	36.4	8.85
3.63	1.21	0.0765	47.5	15.8
4.33	0.972	0.0910	47.6	10.7

表 4: F_1 の因数分解 (初期因子：2 個)

total degree $\simeq$ 40

T_H(秒)	T_W(秒)	T_E(秒)	T_H/T_E	T_W/T_E
16.2	4.07	0.0660	245.	61.7
17.1	4.55	0.0630	271.	72.2
13.5	4.27	0.0590	229.	72.3
27.4	8.53	0.0645	425.	132.
22.5	5.88	0.0690	326.	85.2

total degree $\simeq$ 60

T_H(秒)	T_W(秒)	T_E(秒)	T_H/T_E	T_W/T_E
203.	64.0	0.100	2030.	640.
119.	41.4	0.0915	1300.	452.
203.	71.5	0.108	1880.	662.
196.	51.9	0.116	1690.	447.
198.	60.7	0.0920	2150.	660.

表 5: F_2 の因数分解 (初期因子：4 個)

実験結果を 表 4, 5 に示す。まず初期因子が 2 個である F_1 について、表 4 の結果をみると全次数が 40 次前後の場合は method E に対して method W の計算時間は 2~4 倍、method H では 8~12 倍程度である。全次数が 60 次前後の場合は method W では 8~16 倍、method H では 35~50 倍 になる。

それに対し、初期因子が 4 個である F_2 について、表 5 の結果をみると、計算時間は method E については F_1 とそれほど差がないが、method H, W については F_1 のときより大幅に増加している。F_2 では全次数が 40 次前後の場合 method E に対して method W の計算時間が 60 倍以上、method H では 200 倍以上にもなり、全次数が 60 次前後の場合 method W では 400 倍以上、method H では 1300 倍以上にもなる。

以上より、多項式の全次数が高くなる程 method E と method H, W との計算時間の差が大きくなっていることである。これは、method H, W において平行移動後の多項式の項数の増加も大きくなるためその分、計算時間に上乗せされることがいえる。

元の多項式の多項式因子の個数と一致するときは method W は速く因数分解を行えるが、そうでないときは method W と同様に多項式因子が直接現れず、べき級数として Hensel 因子が計算される。したがって、計算時間にもその影響が現れる。これに対し method E の場合、Hensel 因子は 2 章でも述べたように同次有理式として現れるが、これは拡張 Hensel 構成の計算途中でも組み合わせることで初期因子が多項式因子の個数と異なる場合でも両者が一致する場合と同様に計算できる。以上より、計算時間の差が大きくなっているといえるだろう。

5 まとめと課題

本稿では、主係数問題に対応した拡張 Hensel 構成を用いた多変数多項式の因数分解を実装し、一般 Hensel 構成において非零代入を必要とする多変数多項式因数分解についてその効率性を検証した。このアルゴリズムはまだ初期段階ではあるが、それでも前章の実験の結果より拡張 Hensel 構成において Newton 多角形の下辺が 1 本の場合は一般 Hensel 構成を用いた方法と比べて非零代入を行わないことによる効率性が現れていることが示された。

しかし、拡張 Hensel 構成において Newton 多角形の下辺が 2 本以上の場合、本稿で紹介した方法では効率性が現れてはいない。本稿では Newton 多角形の下辺について $\mathcal{S}_1 \Rightarrow \mathcal{S}_2 \Rightarrow \cdots \Rightarrow \mathcal{S}_\rho$ の一方向のみで Hensel 因子を求めたが、これを逆方向の順で Hensel 因子を求めていく方法もある ([SI00] 参照)。この 2 つを上手く利用することにより、拡張

Hensel 構成の次数を低く抑えることができると思われる。また、各従変数に対し適切な重みを付けて全次数変数を導入することにより Newton 多角形の下辺の数を少なくするように変形させてるという方法もある。また、本稿では拡張 Hensel 構成において Newton 多項式が無平方である場合には工夫が必要である。解決策の 1 つに先ほど述べたが、各従変数に対し適切な重みを付けて全次数変数を導入し、Newton 多項式が無平方になるようにする方法がある。しかし、いずれの方法もまだ実装には至るまでには工夫が必要である。それらを解決していくことが今後の課題といえよう。

参 考 文 献

[Abh89] S. S. Abhyankar: Irreducibility criterion for germs of analytic functions of two complex variables. Adv. in Math., Vol. 74, 190-267 (1980).

[Abh90] S. S. Abhyankar: *Algebraic Geometry for Scientists and Engineers.* Number 35 in Mathematical Surveys and Monographs. Providence, RI: American Mathematical Society.

[KT90] E. Kaltofen and B. M. Trager: Computing with polynomials given by black boxes for their evaluations: greatest common divisors, factorization, separation of numerators and denominators. J. Symb. Comput., Vol. 9, 301-320 (1990).

[Kuo89] T.-C. Kuo: Generalized Newton-Puiseux theory and Hensel's lemma in $\mathbf{C}[[x, y]]$. Canad. J. Math., Vol. XLI, 1101-1116 (1989).

[McC97] S. McCallum: On testing a bivariate polynomial for analytic reducibility. J. Symb. Comput., Vol. 24, 509-535 (1997).

[McD95] J. McDonald: Fiber polytopes and fractional power series. J. Pure and Applied Algebra, Vol. 104, 213-233 (1995).

[MS73] J. Moses and D. Y. Y. Yun: The EZGCD algorithm. *Proc. 1973 ACM National Conference*, ACM, 159-166 (1973).

[Mus71] D. R. Musser: Algorithms for polynomial factorizations. Ph. D. Thesis, University of Wisconsin, 1971.

[SI00] T.Sasaki and D.Inaba: Hensel construction of $F(x, u_1, \ldots, u_l), l \geq 2$, at a singular point and its applications. ACM SIGSAM Bulletin, Vol.34, 2000, pp. 9-17

[SK99] T. Sasaki and F. Kako: Solving multivariate algebraic equation by Hensel construction. Japan J. Indus. Appl. Math., **16**, 257-285 (1999).

[Wan77] P. S. Wang: Preserving sparseness in multivariate polynomial factorization. *Proc. 1977 MACSYMA Users Conference*, MIT, 55-61 (1977).

[WR75] P. S. Wang and L. P. Rothschild, Factoring multivariate polynomials over the integers. Math. Comp., **29**, 935-950 (1975).